Some Interesting Constructions for Secret Sharing Schemes

Diane Donovan

Centre for Combinatorics
Department of Mathematics
The University of Queensland
Brisbane, 4072, Queensland
Australia

Dedicated to the memory of Alan Rahilly, 1947–1992

Abstract: This article documents some of the known constructions for secret sharing schemes. It includes a discussion of the mathematical structures which have been used to model secret sharing schemes, the establishment of secret sharing schemes which do not require the existence of a trusted authority to administer them, variations which can be incorporated into these schemes to increase their flexibility and the detection of cheaters.

1 Introduction and Preliminaries

There are many situations in which it is desirable to restrict access to classified information, or to initiate some action only when certain conditions are met. Examples of such situations are easily found in banking or financial institutions, the military or communication networks which receive encrypted messages. The controlled action can be governed through a secret key and a key management system. This article looks at key management systems which are known as secret sharing schemes. Secret sharing schemes came into prominence in 1979 when two papers, one by Blakley [8] and one by Shamir [42], were published.

A *secret sharing scheme* (SSS) is a method whereby n pieces of information called *shares* or *shadows* are assigned to a *secret key* K in such a way that

1. the secret key can be reconstructed from certain authorised groups of shares, and

2. the secret key cannot be reconstructed from unauthorised groups of shares.

A secret sharing scheme is said to be *perfect* if Item 2 above can be strengthened as follows:

2'. an unauthorised group of shares cannot be used to gain any information about the secret key.

The recipients of the shares are said to be the *participants* in the scheme. An authorised group of participants is a group whose shares can be used to reconstruct the secret. Let the set of participants be $\mathcal{P}$, where $|\mathcal{P}| = n$, and let Γ be a subset of the power set $2^{\mathcal{P}}$. The set Γ is said to be an *access structure* or *concurrence scheme* if the elements of Γ are precisely the authorised groups of participants. The subsets in Γ are termed the *authorised subsets*. In this paper it will be required that given any participant, say P_i, there exists an unauthorised group of participants who can reconstruct the secret once the share of P_i is added to their own. That is, each participant is a necessary part of some reconstruction process. Schemes which satisfy this property have been termed *connected* by Brickell and Davenport [**13**]. The SSSs discussed in this paper all have the property that the keys are selected from a finite set, denoted by $\mathcal{K}$. A discussion of schemes based on an infinite set of keys can be found in [**21**]. The key space $\mathcal{K}$ is made public knowledge and a secret key, K, is chosen from $\mathcal{K}$. Once K is chosen, then a finite set of shares $\mathcal{S}$ is chosen and distributed to the participants in accordance with the scheme.

Let B and C be arbitrary subsets of $\mathcal{P}$. An access structure is said to be *monotone* if whenever $B \subseteq C$ and $B \in \Gamma$, then $C \in \Gamma$. All access structures discussed in this paper are monotone. Non-monotone access structures have been discussed by Beutelspacher in [**7**]. A set $B \in \Gamma$ is said to be a *minimal* authorised subset if, for all $A \subset B$, $A \notin \Gamma$. The set of all minimal authorised subsets, Γ_0, of Γ is said to be the *basis* of Γ. It is now possible to define Γ in terms of the closure of Γ_0; that is, $\Gamma = cl(\Gamma_0) = \{A \subseteq \mathcal{P} \mid B \subseteq A, \text{ where } B \in \Gamma_0\}$. The *rank* of an access structure is defined to be the maximum cardinality of the minimal authorised subset. For a specific example of these concepts, let the set of participants $\mathcal{P}$ be $\{P_1, P_2, P_3, P_4, P_5\}$ and let the access structure be $\Gamma = \{\{P_1, P_3, P_4\}, \{P_1, P_3, P_4, P_2\}, \{P_1, P_3, P_4, P_5\}, \{P_1, P_2, P_4, P_5\}, \{P_2, P_3, P_4, P_5\}, \mathcal{P}\}$. Then the minimal authorised subsets are $\{P_1, P_3, P_4\}, \{P_1, P_2, P_4, P_5\}$ and $\{P_2, P_3, P_4, P_5\}$, and these form the basis Γ_0. The rank is four. This access structure is certainly monotone.

Karnin, Greene and Hellman [**30**] showed that if one chooses the secret to be a number $K \in Z_q$ and the shares to be numbers s_i, $i = 1, \ldots, n$, such that $\sum_{i=1}^{n} s_i = K (\text{mod } q)$, then one has a SSS in which the n participants can jointly determine the secret. This scheme exhibits a high degree of security as $\Gamma = \{\mathcal{P}\}$ and the only way the key can be reconstructed is by combining the information held by all the participants. If $n-1$ participants collaborate each of the possible keys is equally likely to be the secret. However, this also means that if one of the participants is incapacitated the key cannot be recovered. Shamir [**42**] and Blakley [**8**] addressed this problem in 1979 and constructed SSSs in which any t out of the n participants can combine their shares and recover the secret. The access structure of such a scheme consists of any set of t or more participants. An access structure, Γ is defined to be a *threshold access structure* if $\Gamma = \{A \subseteq \mathcal{P} \mid |A| \geq t\}$ and a secret sharing scheme with such an access structure is said to be an *t–out–of–n threshold scheme*. The parameter t is often referred to as the *threshold* of the scheme. Such schemes can withstand

security breaches of up to $t-1$ participants and the secret can still be recovered given that up to $n-t$ pieces of information are lost.

In a perfect threshold scheme the information content of each share must be at least as much as that of the information content of the secret. To see this one begins by assuming that the information content of some share, s_i, held by participant P_i, is less than that of the secret K. In a perfect t–out–of–n threshold scheme the probability of $t-1$ participants, distinct from P_i, collaborating and guessing K is the same as the probability of an outsider guessing K. However, if the $t-1$ participants knew s_i they could recover the secret. The probability of their guessing s_i is greater than the probability of their guessing K, a contradiction. (A proof for general SSSs is similar.)

In 1989 Brickell [**12**] defined the information rate of a SSS. The definition presented below is taken from Stinson [**52**]. Let $\mathcal{K}$ be the key space, and so any secret key K may be represented by a bit string of length $\log_2 |\mathcal{K}|$. Similarly, if $\mathcal{S}_i$ denotes the set of possible shares associated with participant P_i, then the share distributed to participant P_i can be represented by a bit string of length $\log_2 |\mathcal{S}_i|$. The *information rate for participant* P_i is the ratio

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}.$$

The *information rate of the SSS* is denoted by ρ, where

$$\rho = \min\{\rho_i \mid 1 \leq i \leq n\}.$$

The *average information rate* is denoted by $\tilde{\rho}$, where

$$\tilde{\rho} = \frac{|P| \log_2 |\mathcal{K}|}{\sum_{i=1}^{n} \log_2 |\mathcal{S}_i|}.$$

In a perfect SSS $\rho \leq \tilde{\rho} \leq 1$. Therefore the case where $\rho = \tilde{\rho} = 1$ is the best possible information rate and such SSSs are said to be *ideal*.

Many authors have extended the ideas of Blakley and Shamir, and a variety of different constructions for SSSs have been developed. These constructions are discussed in Sections 2 and 3. A discussion of schemes which do not require a trusted authority to administer them is given in Section 4. Sections 5 and 6 deal with systems in which the participants are either partitioned into classes or are members of a hierarchical structure. In most key management systems one must allow for participants who disclose or fraudulently use their shares. Methods for dealing with such situations are discussed in Sections 7, 8 and 9.

Many of the known constructions are similar in nature and instead of listing all methods the reader will be given the general flavour of the ideas and other references mentioned.

2 Threshold Schemes

This section documents some of the known constructions for threshold schemes. Throughout this section it will be assumed that a trusted authority is available to select the secret key and to distribute the shares.

2.1 Geometric configurations

Blakley's original construction, [8], is based on geometric configurations. Since 1979 geometries have figured prominently in the construction of SSSs. See, for example, [6], [15], [38], [44], [45], [46], [47], [48], [49] and [51]. Simmons [47] gives a particularly thorough survey of constructions based on geometries. Therefore, only one small example of a threshold scheme constructed from a projective 4-space will be presented here, followed by a brief description of a general construction. (The reader will find a full discussion of the properties of geometric configurations in [55].)

Take a projective geometry $PG(4, q)$. The key space is taken to be a plane π in $PG(4, q)$. The protocol for a 3–out–of–n threshold scheme is as follows:

Protocol:

- A point p, in π is chosen as the secret key.
- The share space is taken to be a set of points in a plane π_1 chosen such that π_1 and π have a unique point of intersection, p. This set of points must satisfy the properties that no three are collinear and no two lie on a line with p. These points are distributed to the participants as shares.
- When any three participants come together, they can determine π_1, find its point of intersection with π, and recover the secret.

To see that the above scheme is perfect, π is fixed and it is assumed that there is an unauthorised collusion of two participants. The shares of these two participants define a line L which is skew to π. Let q be an arbitrary point in π. There is a unique plane generated by q and L. Denote it by π_2. Assume that this plane intersects π in the line L_1. The lines L_1 and L both belong to the projective plane π_2 and so must intersect in a point. But this would imply that L and π intersect in a point, a contradiction. Thus π and π_2 must intersect in the single point q. Since q was chosen arbitrarily, for each point of π there is a unique plane containing that point and the points held by the two participants. Hence each of the points of π is equally likely to be the secret. Thus the scheme is perfect.

This construction can be generalised as follows. (Note that this particular presentation is taken from Brickell and Stinson [14].) Let V be a t-dimensional vector space over $GF(q)$, where q is some large prime power. The cosets of the subspaces of V form an affine geometry $AG(t, q)$ of dimension t over $GF(q)$. The trusted authority selects a line L in V to be the key space. He then selects a $(t-1)$-dimensional subspace H which meets L in a point. He selects a point p on the line L to be the secret key and constructs the hyperplane $H_p = H + p$. Now he selects points s_i $(1 \leq i \leq n)$ from H_p such that the set of points $\{p\} \cup \{s_i \mid 1 \leq i \leq n\}$ are in general position; that is, no j of the points in the set $\{p\} \cup \{s_i \mid 1 \leq i \leq n\}$ lie on a flat of dimension $j-2$, if $j \leq t$. For $i = 1, \ldots, n$, participant P_i is given the point s_i as his share. When a set of t or more participants come together they can uniquely determine the hyperplane H_p and so obtain the secret key p by calculating $H_p \cap L = p$. However if a subset of t' $(< t)$ participants collaborate their shares generate a flat F of dimension $t'-1$. For any point p' on L there is a hyperplane H' containing F and p'. Hence they have

no information as to the point p. Thus the scheme is a perfect t–out–of–n threshold scheme. It should be pointed out that when the shares are chosen one must check that they are in general position. However, if care is taken when choosing the points then this checking can be avoided.

Simmons [47] and others take the general view that the key space is a subspace V_d of dimension m and the shares are chosen from a subspace V_i which intersects V_d at a point, the secret key. If both V_d and V_i are contained in the space V of dimension v, then V_i can be chosen such that its dimension is $v - m$. Therefore it is not the case that all perfect schemes arising from geometric constructions are ideal.

2.2 Polynomial interpolation

Shamir's original threshold scheme, given in [42], is based on polynomial interpolation of t points in a 2-dimensional plane. Let $f(x)$ be a polynomial of degree at most $t-1$ over the field $GF(q)$. Assume that, for j $(1 \leq j \leq t)$ distinct elements x_j of $GF(q)$, the values of $f(x_j)$ are known. Hence a system of t linearly independent equations

$$f(x_j) = \sum_{i=0}^{t-1} a_i {x_j}^i,$$

in t unknowns, $a_0, \ldots, a_{t-1}$, can be obtained. Lagrange interpolation, (see [25]), can now be used to determine uniquely the t unknowns. So the polynomial can be recovered from the t points. Shamir used this property of polynomial interpolation to construct a t–out–of–n threshold scheme.

For simplicity, take $GF[q]$ to be Z_q, for some large prime q, and let this set be the key space. In Shamir's scheme a secret key K is chosen from Z_q and then a polynomial $f(x)$ of degree $t-1$ with constant coefficient K is also chosen. The participants are labeled $P_1, \ldots, P_n$, where $n \leq q-1$. For $i = 1, \ldots, n$, participant P_i is given the value $f(i)$ as his share. When any t participants come together they can use their shares to recover $f(x)$ and hence K.

Assume that $t-1$ participants wish to collaborate and try to guess the secret. The $t-1$ participants generate a set of $t-1$ equations in t unknowns. These equations have as their solution a set of q polynomials

$$f(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i,$$

where a_0 ranges over all the elements of Z_q. Hence each of the possible keys is equally likely and the scheme is perfect.

From an implementation view point, the generation of the shares simply involves evaluating the polynomial at the n points and then using fast algorithms the key can be recovered in time $O(t \log^2 t)$.

A number of authors have generalised this approach. See for example, Dawson, Mahmoodian and Rahilly [23], Jackson and Martin [29] and McEliece and Sarwate, [36]. Dawson, Mahmoodian and Rahilly base their construction on orthogonal arrays, Jackson and Martin on transversal designs and McEliece and Sarwate on Reed–Solomon codes. Further constructions may also be found in [30], [31], and [33].

2.3 The Chinese Remainder Theorem

Asmuth and Bloom [1] have developed a t–out–of–n threshold scheme from the Chinese Remainder Theorem. They achieve this as follows. A set of integers $\{q, m_1, m_2, \ldots, m_n\}$, where $m_1 < m_2 < \ldots < m_n$, is chosen subject to the following conditions.

- $gcd(q, m_i) = 1$, for all $i = 1, \ldots, n$
- $gcd(m_i, m_j) = 1$, for $i \neq j$ where $i, j = 1, \ldots, n$
- $m_1 m_2 \ldots m_t > q m_{n-t+2} \ldots m_n$

The first two conditions imply that the integers in the set $\{q\} \cup \{m_j \mid j = 1, \ldots n\}$ are pairwise relatively prime. The last condition implies that the product of the t smallest integers from the set $\{m_j \mid j = 1, \ldots n\}$ is greater than the product of q with the $t-1$ largest integers from the set $\{m_j \mid j = 1, \ldots n\}$. From this one can deduce that if $M = m_1 m_2 \ldots m_t$, then M/q is greater than the product of any set of $t-1$ integers from $\{m_j \mid j = 1, \ldots n\}$.

The set Z_q is taken to be the key space and a key $K \in Z_q$ is chosen. The participants are labeled $P_1, \ldots, P_n$. Let A be an integer such that $0 \leq A < M/q$. The trusted authority sets $K_0 = K + Aq$. Note that $0 \leq K_0 < M$. Then, for $i = 1, \ldots, n$, the trusted authority calculates the share $s_i = K_0 \pmod{m_i}$ and distributes this to participant P_i. When any t participants collaborate they can pool their t shares, $s_{j(1)}, \ldots s_{j(t)}$, and then, by the Chinese Remainder Theorem, K_0 is known modulo $M_1 = m_{j(1)} \ldots m_{j(t)}$. Because $M_1 \geq M$ this uniquely determines K_0, and so K is computed by taking $K = K_0 - Aq$.

On the other hand suppose that only $t-1$ shares are known. Then, using the Chinese Remainder Theorem once again, one can compute $K_2 \pmod{M_2}$ where $M_2 = m_{j(1)} \ldots m_{j(t-1)}$. Since $M > qM_2$ and $gcd(M_2, q) = 1$, the collection of numbers $u_i \equiv K_2 \pmod{M_2}$ and $u_i \leq M$ covers all congruence classes modulo q. Thus there is no useful information available without t shares. However, the scheme is not perfect. To see this note that $M - M_2$ is not necessarily divisible by q. Hence the number of u_i's covering a particular integer modulo q varies, and so some values are more likely to be congruent to K_2 modulo q than others. Asmuth and Bloom also describe an efficient algorithm recovering the key K. This algorithm requires only $O(t)$ time.

A similar approach is taken by Mignotte in [37] and an example of this construction can be found in Denning [25] on page 183.

2.4 Block designs

Another structure used in the construction of threshold schemes is that of a block design. Let V be a finite set of v elements and $\mathcal{B}$ a family of k–subsets of V. The elements of $\mathcal{B}$ are sets of size k, termed *blocks*. If each t element subset of V occurs in λ blocks of $\mathcal{B}$, then $\mathcal{B}$ constitutes a *t–design* with parameter set t–(v, k, λ). A *Steiner system* is a t–design with $\lambda = 1$, and is usually denoted by $S(t, k, v)$.

There are two known constructions using t–designs. In the first construction, Beutelspacher and Vedder [6] and Beutelspacher [5], take a $S(t,k,v)$ Steiner system and construct a t–out–of–n threshold scheme, where $n \leq k$, as follows. The blocks of the design are ordered 1 through b and this ordering is made public knowledge. A number $K \in \{1,\ldots,b\}$ is chosen as the key. The block corresponding to this number is selected and the elements of this block are distributed to the participants as shares. When t participants come together their shares determine a unique block. This block has been assigned the number K. So, they may recover the key. However, the scheme is not perfect. If $t-1$ participants come together, there are $(v-t+1)/(k-t+1)$ blocks which contain their shares. Hence the probability of their guessing the secret is $(k-t+1)/(v-t+1)$, whereas the probability of an outsider guessing the secret is $1/b$, where $b = \left(\begin{array}{c} v \\ t \end{array}\right) / \left(\begin{array}{c} k \\ t \end{array}\right)$.

Stinson and Vanstone [50] have shown that it is possible to construct perfect threshold schemes from Steiner systems. (See also [19], [40] and [53].) In some cases it is possible to partition a $S(t,k,v)$ Steiner system into $m = (v-t+1)/(k-t+1)$ disjoint $S(t-1,k,v)$ Steiner systems. This partition has the property that any t–subset of V occurs in precisely one design of the partition. In addition, each $(t-1)$–subset occurs in a block of every design of the partition, since each design is a $S(t-1,k,v)$. An example of a $S(3,3,9)$ Steiner system which has been partitioned into seven $S(2,3,9)$ Steiner systems is given in Table 2.4.1.

In order to construct a perfect t–out–of–n threshold scheme, a partition of a $S(t,k,v)$ Steiner system into $m = (v-t+1)/(k-t+1)$, $S(t-1,k,v)$ Steiner systems is taken. The set $\{1,\ldots,m\}$ is taken to be the key space and each $S(t-1,k,v)$ Steiner system is assigned a value i, for $i = 1,\ldots,m$. The key space and the assignment is made public knowledge. The protocol for a t–out–of–k threshold scheme is as follows.

Protocol:

- A number $K \in \{1,\ldots,m\}$ is chosen to be the secret key.
- The $S(t-1,k,v)$ Steiner system corresponding to K is located and a block of that design is chosen. The elements of this block are distributed as shares.
- When any t participants come together, they pool their shares and locate the unique block, of the $S(t,k,v)$ Steiner system, containing their shares. This block belongs to a unique Steiner system with parameters $S(t-1,k,v)$, and this system corresponds to one of the values $1,\ldots,m$. The secret key K is the number $i \in \{1,\ldots,m\}$ corresponding to the appropriate $S(t-1,v,k)$.

Consider an unauthorised set of $t-1$ participants collaborating. They hold $t-1$ shares. Each of the Steiner systems with parameters $S(t-1,k,v)$ contains a unique block on these shares. Hence the probability of the $t-1$ participants guessing the secret is the same as an outsider, $1/m$. Therefore the scheme is perfect.

As an example one may take the partition given in Table 2.4.1 and construct a 3–out–of–3 threshold scheme as follows. Here, the $S(3,3,9)$ is partitioned into $m = 7$

Steiner systems with parameters $S(2,3,9)$, and these are assigned the values $1,\ldots,7$, respectively.

S_1	S_2	S_3	S_4	S_5	S_6	S_7
1 2 3	1 2 4	1 2 5	1 2 6	1 2 7	1 2 8	1 2 9
1 4 9	1 3 9	1 3 7	1 3 8	1 3 5	1 3 6	1 3 4
1 5 7	1 5 8	1 4 8	1 4 7	1 4 6	1 4 5	1 5 6
1 6 8	1 6 7	1 6 9	1 5 9	1 8 9	1 7 9	1 7 8
2 4 7	2 3 6	2 3 4	2 3 9	2 3 8	2 3 7	2 3 5
2 5 8	2 5 7	2 6 8	2 4 5	2 4 9	2 4 6	2 4 8
2 6 9	2 8 9	2 7 9	2 7 8	2 5 6	2 5 9	2 6 7
3 4 8	3 4 5	3 5 6	3 4 6	3 4 7	3 4 9	3 6 8
3 5 9	3 7 8	3 8 9	3 5 7	3 6 9	3 5 8	3 7 9
3 6 7	4 6 8	4 5 9	4 8 9	4 5 8	4 7 8	4 5 7
4 5 6	4 7 9	4 6 7	5 6 8	5 7 9	5 6 7	4 6 9
7 8 9	5 6 9	5 7 8	6 7 9	6 7 8	6 8 9	5 8 9

TABLE 2.4.1

Table 2.4.1 together with the key space $\{1,\ldots,7\}$ is made public knowledge. A number is chosen at random from the set $\{1,\ldots,7\}$ and taken to be the secret key. Assume it is 4. A block is chosen from S_4, say the block $\{2,7,8\}$. The elements of this block are distributed to the three participants as shares. When the three participants come together, they can locate the unique block containing their shares. This block belongs to precisely one Steiner system with parameters $S(2,3,9)$, namely S_4. Therefore, the secret key is $K=4$. It is easy to see that this scheme is perfect since the shares held by any two participants belong to a block in each of the Steiner systems with parameters $S(2,3,9)$.

The general scheme presented here is not ideal as the shares are selected from a set of size v and the key space is of order $|\mathcal{K}| = (v-t+1)/(k-t+1)$. However, if one uses this construction to develop an *anonymous threshold scheme*, (see Stinson [**53**] for a definition), then it can be shown that the number of keys is optimal in this model. In addition the structure of Steiner systems places severe restrictions on the possible parameters for the associated access structure. Finally, the scheme is difficult to implement, when $t \geq 3$, as there are not many known examples of partitionable Steiner systems.

Dawson, Mahmoodian and Rahilly [**23**] have a similar construction based on a partition of an orthogonal array. The advantages of this scheme are that it is ideal, the parameter set is more flexible and there are many more known examples. In fact this construction turns out to be a generalisation of Shamir's scheme and has been mentioned briefly in Section 2.2.

3 Secret Sharing Schemes For General Access Structures

In a *general SSS* the access structure is not restricted to a set of t or more participants. Instead, it is a collection of authorised subsets of participants. In 1987 Ito, Saito and Nishizeki [28] generalised Shamir's construction and designed a SSS which realises any given access structure. Basically, they take a polynomial $y = f(x)$, of degree $t-1$, and take the secret to be $f(0)$. The polynomial is evaluated at m points $(x_1, y_1), \ldots, (x_m, y_m)$ and these points are taken to be the set S. Each participant P_i, for $i = 1, \ldots, n$, is assigned a set of shares $D_i \subset S$. A group of participants can recover the secret if the union of their sets covers at least t points of S. Ito, Saito and Nishizeki termed their scheme a multiple assignment scheme and formalised these ideas as follows: The key space is taken to be $GF(q)$, where q is a prime power.

Protocol:

- Two integers t and m are chosen such that $t \leq m < q$ and a secret key K is chosen from $GF(q)$.
- Elements $a_1, \ldots, a_{t-1} \in GF(q)$ and $a_{t-1} \in GF(q) \backslash \{0\}$ are randomly chosen, and taken as the coefficients of the polynomial $f(x) = K + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$.
- Distinct elements $x_1, \ldots, x_m$ are chosen from $GF(q) \setminus \{0\}$ and $y_i = f(x_i)$ is calculated.
- Let $S = \{(x_1, y_1), \ldots, (x_m, y_m)\}$ and label the participants $P_1, \ldots, P_n$. For $i = 1, \ldots, n$, sets $D_i \subset S$ are chosen and participant P_i is assigned D_i as his share.
- The key can be recovered when a set $A = \{P_{i(1)}, \ldots P_{i(j)}\}$ of participants come together such that $|\cup_{P_i \in A} D_i| \geq t$.

The assignment of the shares is taken to be the function $g : \mathcal{P} \rightarrow 2^S$ such that $g(P_i) = D_i$ and this assignment scheme has the access structure

$$\Gamma = \{Q \subset \mathcal{P} \mid |\cup_{P \in Q} g(P)| \geq t\}.$$

They proved that any monotone access structure can be realised using the above techniques. It is also clear that the resulting scheme is perfect. The proof of this result follows that given in Section 2.2. These ideas were taken up by Benaloh and Leichter in [3]. They gave a simpler and more efficient method for developing a SSS for any monotone access structure. Essentially, a key K is chosen and for each set B of the access structure, $|B|$ values $s_1, \ldots, s_{|B|}$ are selected such that the sum $s_1 + \ldots + s_{|B|} = K$. If at some stage it is possible to combine sets in the access structure to form a t_i–out–of–n_i threshold scheme, then an intermediate value s_i can be divided into n_i shares any t_i of which will recover s_i. In this manner, Benaloh and Leichter reduced the number of shares to be held by any one participant. However, they also point out that it is not always possible to construct a scheme in which each participant receives only one share. This fact can be established by considering the

access structure with basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$. Consequently, they showed that an ideal scheme does not exist for the access structure with basis Γ_0.

To help study general access structures Benaloh and Leichter [3] also introduced terminology which can be used to give a concise method for representing a monotone access structure. This terminology was later adapted by Brickell and Stinson [15], Stinson [51] and Simmons, Jackson and Martin [48]. An in depth discussion of this terminology can be found in [51]. Briefly, each participant P_i is assigned a variable x_i and the access structure is represented by a formula of the form

$$\bigvee_{B \in \Gamma} \left(\bigwedge_{x_i \in B} x_i \right),$$

where the x_i's take a true or false value. The value of the formula is true if and only if the set of variables which are true correspond to a subset of $\mathcal{P}$ which is in the access structure. The formula is termed a *monotone formula* or a *monotone circuit*. For example, an access structure with basis $\{\{P_1, P_2\}, \{P_2, P_3, P_4\}\}$ can be represented by the monotone formula $(x_1 \wedge x_2) \vee (x_2 \wedge x_3 \wedge x_4)$.

Quite a deal of research has been conducted into methods which can be used to realise general monotone access structures. Some of these methods are discussed in detail below, other constructions can be found in [22] and [34].

3.1 Geometric configurations

Since geometric constructions have been discussed by a number of authors (see for example Simmons [47], [45] and [46]) only one small example will be given here. Consider the access structure with basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_3, P_4\}\}$. Take the key space to be the set of points in a subspace V_d of an affine space. A point p is taken to be the secret key. The shares are taken from a plane π which intersects the subspace in the unique point p. Participants P_1 and P_2 receive points on a line which is in π and contains p. Participant P_3 receives a line in π which does not contain p and P_4 a point in π and not on the lines already chosen. It is easy to see that together P_1 and P_2 can recover a line which intersects the subspace at p and P_3 together with any one of the other three participants can recover the plane π and hence the unique point p.

Simmons, Jackson and Martin [48] discussed the realisation of SSSs, based on geometric configurations, for general access structures. In this paper, they point out that even very simple access structures may require fairly complicated geometric configurations for their realisation. However, they present an algorithm for achieving this. They then apply these techniques and use geometric constructions to realise SSSs for all possible access structures on four or fewer participants.

3.2 Vector spaces

Constructions using vector spaces are closely related to those based on geometry. One such construction, taken from Brickell [12], is given here. Let Γ be an access

structure. Let V be a vector space of all d–tuples over $GF(q)$, where q is some prime power and $d \geq 2$. The key space is taken to be $GF(q)$. Note that below $\cdot$ is the inner product of $GF(q)$. The protocol for a general SSS based on access structure Γ is given below.

Protocol:

- A secret key $K \in GF(q)$ is chosen, and a vector $\overline{a} = (a_1\, a_2 \ldots a_d)$ is chosen in such a way that $K = \overline{a} \cdot (1\ 0 \ldots 0)$.
- The share space is taken to be $GF(q)$. The participants are labeled $P_1, \ldots, P_n$, and participant P_i is assigned a vector v_i. For $i = 1, \ldots, n$, the vectors, v_i, are chosen in such a way that $(1\ 0 \ldots 0)$ belongs to the span of the set $\{v_i \mid P_i \in A\}$ if and only if $A \in \Gamma$. For $i = 1, \ldots, n$, the share distributed to participant P_i is the value $s_i = \overline{a} \cdot v_i$.
- An authorised group of participant can recover the secret key K by taking the summation $\sum_{i|P_i \in A} w_i s_i$, where each $w_i \in GF(q)$. (Note that the values w_i can be precomputed and stored.)

To prove that an authorised group can recover the secret, one proceeds as follows. Recall that the shares are chosen in such a way that $(1\ 0 \ldots 0)$ belongs to the span of the set $\{v_i \mid P_i \in A\}$ if and only if $A \in \Gamma$. Therefore,

$$(1\ 0 \ldots 0) = \sum_{i|P_i \in A} w_i v_i.$$

Now, $\overline{a}$ is also chosen so that $\overline{a} \cdot (1\ 0 \ldots 0) = K$. Hence

$$K = \overline{a} \cdot \sum_{i|P_i \in A} w_i v_i = \sum_{i|P_i \in A} w_i\ \overline{a} \cdot v_i.$$

The shares s_i are chosen so that $s_i = \overline{a} \cdot v_i$. Therefore

$$K = \sum_{i|P_i \in A} w_i s_i.$$

It can be shown that this scheme is perfect. For a proof of this see Brickell's original paper or Stinson [51]. It is easy to see that this scheme is also ideal.

Benaloh and Leichter [3] showed that there exist monotone sets Γ, which cannot be the access structure of an ideal SSS. (See also Wallis [58].) Therefore this construction cannot be used to realise SSSs for all possible access structures. Also it should be noted that in general there is no known efficient algorithm for finding vectors v_i which satisfy the given conditions.

A similar construction is given by Bertilsson and Ingemarsson in [4].

3.3 Matroids

Matroids have played a significant role in the realisation of general access structures.

A *matroid* $\mathcal{M}$ is a pair $(V, \mathcal{I})$, where V is a non–empty finite set and $\mathcal{I}$ is a non–empty collection of subsets of V, called *independent sets*, which satisfy the following properties:

1. any subset of an independent set is independent;

2. if X and Y are independent sets with $|Y| > |X|$, then there is an element e contained in Y, but not in X, such that $X \cup \{e\}$ is an independent set.

If $\mathcal{M} = (\mathcal{V}, \mathcal{I})$ is a matroid defined as above, then a subset of V is said to be a *dependent set* if it is not independent. A minimal dependent set is called a *circuit*. Let x, y, z be distinct elements of V. A matroid is said to be *connected* if, whenever there are circuits, C_1 containing x and y and C_2 containing y and z, then there exists a circuit C_3 containing x and z. Let F be a field and F^d be a d–dimensional vector space over F. A matroid $\mathcal{M} = (\mathcal{V}, \mathcal{I})$ is said to be *representable* over F if there exists a dependence preserving mapping $g : V \rightarrow F^d$, such that a subset $A \subseteq V$ is a dependent set of the matroid $\mathcal{M}$ if and only if $g(A)$ is linearly dependent. For more details on matroids see Welsh [**57**].

Brickell and Davenport [**13**] were able to show that matroids provide a partial classification of ideal SSSs. To prove this they introduced the following terminology. Let Ω be an ideal SSS with a connected monotone access structure Γ. Let D denote the trusted authority who is administering the scheme. Define $X = \{D\} \cup \mathcal{P}$. The trusted authority is taken to be a participant and it is assumed that he is assigned the key as his share. Given a set $Y \in X$ the notation $Y \setminus \{y\} \Longrightarrow y$ indicates that the shares held by the participants of $Y \setminus \{y\}$ can be used to uniquely determine the share held by participant y. For any SSS Ω let $D(\Omega)$ be the set

$$D(\Omega) = \{A \subseteq \mathcal{P} \mid \exists y \in A \text{ s.t. } (\mathrm{A} \setminus \{\mathrm{y}\} \Longrightarrow \mathrm{y})\}.$$

Brickell and Davenport's partial classification is as follows.

THEOREM 3.1 *Let Ω be a connected ideal SSS. Then the sets $D(\Omega)$ are the dependent sets of a connected matroid.*

THEOREM 3.2 *Let $\mathcal{M}= (V, \mathcal{I})$ be a connected matroid representable over a field. Let $v_0 \in V$. Then there exists a connected ideal SSS Ω such that $K = v_0$, $X = V$ and where $D(\Omega)$ are the dependent sets of $\mathcal{M}$.*

Jackson and Martin [**29**] have extended these two results and established the uniqueness of the matroid in Theorem 3.1 and the access structure associated with the SSS in Theorem 3.2.

Using these results Beimel and Chor [**2**] introduced the idea of appropriate matroids. Let Γ be an access structure on a set of n participants $\{P_1, \ldots, P_n\}$ and let $\mathcal{M} = (\mathcal{V}, \mathcal{I})$, where $V = \{0, 1, \ldots, n\}$, be a connected matroid. The matroid $\mathcal{M}$ is said to be appropriate for the access structure Γ if

$$\Gamma = cl(\{C \setminus \{0\} \mid 0 \in C \text{ and } C \text{ is a minimal dependent set of } \mathcal{M}\}).$$

In other words, the minimal sets of the access structure Γ correspond to the minimal dependent sets containing the element 0 of the matroid. They then went on to define universally ideal access structures and gave a characterisation of these structures. Let

$\mathcal{K}$ be the key space, and $\mathcal{S}_i$ the share space for participant P_i. A SSS is defined to be *m–ideal* if $|\mathcal{K}| = |\mathcal{S}_1| = \ldots = |\mathcal{S}_n| = m$, and an access structure Γ is *m–ideal* if there exists an m–ideal SSS that realises Γ. An access structure Γ is *universally ideal* if for every positive integer m the access structure Γ is m–ideal.

Beimel and Chor showed that an access structure Γ is 2–ideal if and only if there is a matroid which is representable over $GF(2)$ and is appropriate for Γ. Similarly, they showed that an access structure Γ is 3–ideal if and only if there is a matroid which is representable over $GF(3)$ and is appropriate for Γ. They then used the fact that a matroid $\mathcal{M}$ is representable over $GF(2)$ and $GF(3)$ if and only if $\mathcal{M}$ is representable over any field, to show that if an access structure Γ is 2–ideal and 3–ideal then for every q such that q is a power of a prime, Γ is q–ideal. This then led to their main result:

THEOREM 3.3 *An access structure Γ is universally ideal if and only if Γ is 2–ideal and 3–ideal.*

The connection between non-perfect SSSs and matroids has been studied by Kurosawa, Okada and Sakano [32], and Seymour [41] has proved that a certain class of matroids (Vamos matroids) cannot be the associated matroid of an ideal SSS.

3.4 Graphs

A number of authors have used graphs as a way of representing access structures of rank two. The earliest reference to these ideas is Brickell and Davenport [13]. Let $G = (V, E)$ be a connected undirected graph. Each participant is assigned a vertex of G and any two participants can compute the key, if their corresponding vertices are joined by an edge in G. So the access structure consists of the closure of a connected graph. For example, the access structure defined by the basis set $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$ can be represented by the graph given on the left in Figure 3.4.1 and the access structure with basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_3, P_4\}\}$ can be represented by the graph given on the right in Figure 3.4.1.

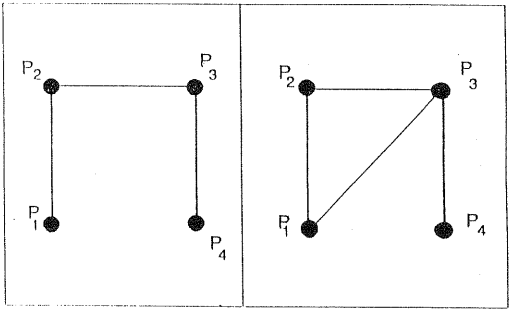

FIGURE 3.4.1

The following result is taken from [13], and can also be found in [15] and [51].

THEOREM 3.4 *Suppose $G = (V, E)$ is a connected graph. Then there is an ideal SSS realising the access structure $\Gamma(G)$ if and only if G is a complete multipartite graph.*

Blundo, De Santis, Stinson and Vaccaro [10] showed that if G is not a complete multipartite graph, then any SSS for G must have an information rate ρ less than or equal to 2/3.

Brickell and Stinson [15] proved the following about the information rate of such SSSs.

THEOREM 3.5 *Suppose $G(V, E)$ is a graph in which the maximum degree of any vertex is d. Then there is a SSS, where the key space is of size q, for some prime q greater than or equal to 2, which realises the access structure $\Gamma(G)$ associated with the graph, and with information rate $\rho = 1/(\lceil \frac{d}{2} \rceil + 1)$.*

Recently, Stinson [54] improved on this result and showed that there exists a SSS satisfying the above conditions and with information rate $\rho \geq 2/(d+1)$.

Brickell and Stinson [15] consider all possible graphs on at most four vertices and show that they all admit ideal SSSs with the exception of two. The two exceptions are given in Figure 3.4.1, and are dealt with in detail in a paper by Capocelli, De Santis, Gargano and Vaccaro [16]. The optimal information rate and the average information rate has been determined for all access structures on at most four participants, for details of these results see [10], [15], [16] and [51]. The optimal information rate and the average information rate has been determined for all graph access structures on at most five participants, for details of these results see [10], [52] and [54]. Blundo, De Santis, Gargano and Vaccaro [11] have exhibited a class of graphs for which upper bounds on the optimal information rate can be shown to become arbitrarily close to 1/2 and upper bounds on the average information rate can be shown to become arbitrarily close to 2/3.

Many of the proofs of these results in this section use what is known as a decomposition construction. This method of construction is discussed in the next subsection.

3.5 Decomposition Construction

Recursive constructions have been used to construct SSSs. These constructions take a basis Γ_0 and decompose it into access structures for which there exist ideal schemes. These ideal schemes are then used as the building blocks for SSS on Γ_0. This method of construction was used by Brickell and Stinson [15]. Then Blundo, De Santis, Stinson and Vaccaro [10] extended Brickell and Stinson's construction and recently Stinson [51] generalised the construction further. The general construction is presented below.

Let Γ be an access structure with basis Γ_0. Let $\mathcal{K}$ be a specified key space. An *ideal decomposition* of Γ_0 consists of a set $\{\Gamma_1, \ldots, \Gamma_m\}$ such that the following properties are satisfied:

1. $\Gamma_k \subseteq \Gamma_0$, for $1 \leq k \leq m$,
2. $\cup_{k=1}^{m} \Gamma_k = \Gamma_0$, and

3. for $1 \leq k \leq m$, there exists an ideal scheme with key space $\mathcal{K}$, on the subset of participants $\mathcal{P}_k = \cup_{B \in \Gamma_k} B$, for the access structure having basis Γ_k.

Stinson points out that in most cases a decomposition can be found such that the set $\{\Gamma_1, \ldots, \Gamma_m\}$ partitions Γ_0.

Stinson formalises the distribution of shares to participants in a SSS as a distribution rule. A *distribution rule* is a function f from participants to shares, and represents a possible distribution of shares to the participants.

The decomposition construction for a SSS on an access structure Γ with basis Γ_0 is given as follows. Let the key space be $\mathcal{K}^l$. Assume that, for $1 \leq j \leq l$,

$$\{\Gamma_{j,1}, \ldots, \Gamma_{j,m_j}\}$$

is an ideal decomposition of Γ_0. Note that by the definition of an ideal decomposition it follows that, for $1 \leq j \leq l$ and $1 \leq k \leq m_j$, there exists an ideal scheme on the subset of participants

$$P_{j,k} = \cup_{B \in \Gamma_{j,k}} B$$

for the access structure with basis $\Gamma_{j,k}$. Let $\mathcal{F}_{K_j}^{j,k}$ denote the set of distribution rules for the corresponding ideal scheme with secret key K_j. A key $(K_1, \ldots, K_l)$ is selected from $\mathcal{K}^l$. Then, for $1 \leq j \leq l$, $1 \leq k \leq m_j$, a distribution rule $f^{j,k} \in \mathcal{F}_{K_j}^{j,k}$ is chosen and this rule is used to distribute the shares to the participants in $\mathcal{P}_{j,k}$.

To calculate the information rate of the scheme with basis Γ_0 one must determine the number of shares distributed to participant P_i. For each participant P_i and for $1 \leq j \leq l$, the number of shares given to P_i for the schemes with distribution rules $\mathcal{F}^{j,k}$, $1 \leq k \leq m_j$, is

$$|\{k \mid P_i \in \mathcal{P}_{j,k}\}|.$$

So in total participant P_i is given

$$R_i = \sum_{j=1}^{l} |\{k \mid P_i \in \mathcal{P}_{j,k}\}|$$

shares.

These calculations may now used to prove the following result.

THEOREM 3.6 *Let Γ be an access structure having basis Γ_0. For $1 \leq j \leq l$, suppose*

$$\{\Gamma_{j,1}, \ldots, \Gamma_{j,m_j}\}$$

is an ideal decomposition of Γ_0 where $\mathcal{P}_{j,k}$ denotes the participant set for the access structure $\Gamma_{j,k}$. Define

$$R = \max\{\sum_{j=1}^{l} |\{k : P_i \in \mathcal{P}_{j,k}| : 1 \leq i \leq n\}.$$

Then $\rho^*(\Gamma) \geq l/R$, where ρ^* denotes the maximum possible information rate for a given access structure.

Stinson [51] illustrates this construction with the following example. Let Γ be an access structure with basis $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\}$. (See Figure 3.4.1 for a graphical representation of this access structure.) Take $l = 2$, $\mathcal{K} = GF(q)$ for any prime power q, and define the two ideal decompositions to be:

$$\begin{aligned}
\Gamma_{1,1} &= \{\{P_1, P_2\}\} \\
\Gamma_{1,2} &= \{\{P_2, P_3\}, \{P_3, P_4\}\} \\
\Gamma_{2,1} &= \{\{P_1, P_2\}, \{P_2, P_3\}\} \\
\Gamma_{2,2} &= \{\{P_3, P_4\}\}.
\end{aligned}$$

Then $R_1 = R_4 = 2$ and $R_2 = R_3 = 3$. Hence $R = 3$ and $\rho = 2/3$.

4 Democratic Schemes

In many situations it is unlikely that there will be an administrator who is trusted by all parties and is capable of establishing and maintaining a SSS. Thus there is a real need to design a *democratic scheme*, in which the participants jointly determine the secret key. To achieve this the participants each select a secret partial key, and these are fed into some initialisation mechanism which determines the secret key. To avoid confusion this secret key will be termed the master key. Each partial key must play a vital role in determining the master key. When the master key is required an authorised group of participants must input pieces of information and these are used to determine first the partial keys and ultimately the master key. In the schemes discussed in the first three sections of this paper the secret key has been determined by a trusted authority who administers the scheme. In a democratic scheme the master key is determined by the inputs of the participants.

Ingemarsson and Simmons [27] were the first to discuss democratic schemes and proposed a number of methods for implementing the above ideas. One simple method suggested by Ingemarsson and Simmons is to have each participant select a number and then the master key is taken to be the sum of these numbers. Alternatively, if there are n participants, each participant might select a hyperplane in an n–dimensional finite space and the master key is taken to be the intersection of these hyperplanes. A full discussion of these ideas can be found in [27]. Ingemarsson and Simmons also gave the following example of a 2–out–of–3 democratic scheme based on a projective 3-space $PG(3, q)$. Label the participants P_1, P_2 and P_3. Take a $PG(3, q)$.

Protocol:

- For $i = 1, 2, 3$, participant P_i chooses a plane π_i, in $PG(3, q)$, as his partial key.
- The planes are fed into an initialisation mechanism and their intersection taken. Let the intersection be p. Then p is taken to be the master key.
- Participant P_i chooses two distinct lines L_i and L_i' in π_i. Note that these lines should not intersect at p. He then distributes a line to each of the other

participants as a share in his partial key. This distribution rule is summarised in Table 4.1. Here the entry in the cell (P_i, P_j) represents the share that participant P_i distributes to participant P_j.

	P_1	P_2	P_3
P_1	π_1	L_1	L'_1
P_2	L_2	π_2	L'_2
P_1	L_3	L'_3	π_3

TABLE 4.1

- When any two participants come together they hold their own planes and two lines in the plane of the third participant. Therefore, they can determine the third plane, take the intersection of the three and recover the point p.

Ingemarsson and Simmons also proposed a more general democratic scheme based on Maximum Distance Separable codes. Dawson and Donovan [24] have given an analogous construction based on Shamir's scheme. This section is concluded with a discussion of this construction. The key space is taken to be Z_q, for some large prime q. The participants are labeled P_1 to P_n, where $n \leq q-1$. A t–out–of–n democratic scheme is presented below.

Protocol:

- Each participant P_i selects a partial key K_i and a polynomial $f_i(x)$ of degree $t-1$ with constant coefficient K_i.
- The master key K is determined by an initialisation process. For example, this initialisation process could involve taking $K = (\sum_{i=1}^{n} K_i) \pmod q$.
- For $i = 1, \ldots, n$, each participant P_i derives $n-1$ shares by evaluating $f_i(j)$, for $j = 1, \ldots, n$ and $j \neq i$.
- Participant P_i distributes the share $f_i(j)$ to participant P_j. (Note that at this step participant P_j holds his own partial key K_j and $n-1$ shares of the form $f_i(j)$ for $i = 1, \ldots, n$ and $i \neq j$.)
- When it is necessary to recover the secret, t or more participants combine their shares. In doing so they derive the n polynomials $f_i(x)$, for $i = 1, \ldots, n$, and hence the n constant coefficients K_i. Now they can recover the key K.

One can see that in a democratic scheme the risk of a security breach is no more than that of an autocratic scheme (one administered by a trusted authority).

5 Multilevel or Hierarchical Schemes

A *multilevel* or *hierarchical access structure* has been defined as one in which the participants are partitioned into levels l_i, for $i = 1, \ldots, R$ and the access structure

consists of those subsets which contain at least r participants all of level at most l_r. A multilevel or hierarchical scheme is one which realises a multilevel access structure.

Shamir [42] addresses this situation in his original paper. He suggests that participants at a lower level be given more shares. (Such schemes have been termed *intrinsic*.) However, this increases the size of the shares and thus the information rate of the scheme is low. In an *extrinsic* scheme the participants' differing capabilities when reconstructing the secret are a function of the relationship between the shares and not a function of the information content of the shares.

Simmons [45] gives the following example of a multilevel scheme which is extrinsic. Take a projective space $PG(4, q)$. The key space is the set of points on a line L in $PG(4, q)$. The protocol for a multilevel scheme is as follows.

Protocol:

- A point p on the line L is chosen to be the secret key K.
- The participants are divided into two levels, denoted by l_2 and l_3.
- A line L_2, which intersects L at p, is chosen. The points, distinct from p, are distributed one to each of the participants in level l_2.
- A plane π_3 which contains L_2, but not L, is chosen. The points in $\pi_3 \setminus L_2$, no two of which are collinear with a point on L_2, are distributed one to each of the participants in level l_3.
- When any two participants from l_2 come together they can determine L_2 and hence the point of intersection with L. When any three participants from l_3 come together they can determine π_3 and hence the point of intersection with L. If one participant from level l_2 and two participants from l_3 come together they can determine π_3 and hence its intersection with L. Thus the secret key K can be determined.

It is easy to see that any pair of participants at level three can replace the share of any participant at level two.

Brickell [12] uses the vector space construction given in Section 3.2 to construct an ideal multilevel scheme. The protocol for the scheme is the same except that, for $i = 1, \ldots, n$, participant P_i is assigned a level L_i and this level is used to choose the vector v_i. For each participant P_i an element $x_i \in GF(q)$ is chosen and the vector v_i is taken to be the l_R–dimensional vector

$$(1, x_i, x_i^2, \ldots, x_i^{L_i - 1}, 0, \ldots, 0).$$

(It should be noted that if $l_1 = 1$ and P_i is a participant with $L_i = 1$, the $v_i = e_1 = (1, 0 \ldots, 0)$.) Then set

$$f_j(x) = \sum_{k=0}^{j-1} a_k x^k$$

and distribute $s_i = f_{L_i}(x_i)$ to participant P_i as his share.

Brickell goes on to give two general theorems (stated below) on the existence of SSSs which realise these multilevel access structures, as well as methods for picking the x_i which are necessary in the construction of the schemes.

THEOREM 5.7 *Let Γ be a multilevel access structure with levels $l_1 < \ldots < l_R$. Let N_r denote the number of participants of level l_r and let n be the total number of participants. If $q > (l_R - 1)\binom{n}{l_R - 1}$, then there is an ideal secret sharing scheme for Γ over $GF(q)$.*

THEOREM 5.8 *Let Γ be a multilevel access structure with levels $1 = l_0 < l_1 < \ldots < l_R$. Let N_r denote the number of participants of level l_r and let n be the total number of participants. Let q be a prime satisfying $q > N_r + 1$ for $1 \leq r \leq R$. Let $\beta = Rl_R^2$. Then there is an ideal SSS for Γ over $GF(q^\beta)$ which can be constructed in time polynomial in $(N_1, \ldots, N_R, q)$.*

Brickell also notes that from an implementation point of view the method of construction used in the first theorem requires the checking of possibly exponentially many matrices to verify that they are nonsingular. However, this problem is overcome if one uses the construction given in the second theorem.

Other references which deal with the construction of multilevel schemes are [5], [6], [12], [31], [22], [24] and [45].

6 Multipart or Compartmented Schemes

In a *multipart* or *compartmented scheme* the participants are divided into several compartments and the shares distributed to the participants in such a way that the secret can be recovered only when at least the prescribed number of participants from each compartment concur. If a quorum is not reached in any one compartment, then the key cannot be reconstructed. Formally, Brickell [12] defines the access structure of a compartmented scheme as follows. Let the sets of participants $C_1, \ldots, C_u$ partition $\mathcal{P}$ and determine integers $t_i \geq 1$, for $i = 1, \ldots, u$. The access structure of a compartmented scheme is made up of the sets $C \in 2^{\mathcal{P}}$ which satisfy the following properties,

1. $|C \cap C_i| \geq t_i$, for $i = 1, \ldots, u$, and
2. $|C| \geq t$.

In the paper [45] Simmons looks at the construction of compartmented schemes from geometric configurations. The following example of a perfect 2–out–of–3 compartmented scheme is taken from that paper. This construction relies on the existence of a projective space $PG(4, q)$, and the fact that any pair of skew lines in $PG(4, q)$ will span a unique 3–dimensional subspace. An arbitrary line L in the $PG(4, q)$ is taken to be the key space. The classes of participants are labeled C_1, C_2 and C_3. The protocol for a compartmented scheme consisting of three groups is given below.

Protocol:

- A point, p, on the line L is chosen to be the secret key K.

- A subspace V of $PG(4,q)$ is chosen such that V intersects L at the point p. A line ω on p and in V is chosen. Three lines L_1, L_2 and L_3 are chosen in V such that they are pairwise skew and each, respectively, intersects ω in the points p_1, p_2 and p_3. The points p_1, p_2 and p_3 must all be distinct from p.

- For $i = 1, 2, 3$, the points on L_i, distinct from p_i, are distributed to the participants in class C_i as their shares.

- When any two participants from class C_i come together they can determine the line L_i.

- When any two classes come together, and obtain a quorum within each class, they determine a pair of skew lines which can be used to generate V. Having obtained V, its intersection with L is taken and $K = p$ recovered.

The proof that the scheme is perfect may be found in [45] and it is easy to see that this scheme is ideal.

Brickell proves that for any compartmented access structure Γ, as defined above, there exists a Q, such that for $q > Q$, there exists an ideal SSS for Γ over $GF(q)$. More precisely Brickell gives the following theorem.

THEOREM 6.9 *Let Γ be a compartmented access structure. If $q > \binom{n}{t}$, then there is an ideal SSS for Γ over $GF(q)$.*

However, Brickell also points out that in general no efficient method for implementing this scheme has been found. In the special case where t is equal to the sum of the t_i's Brickell suggests that, for $i = 1, \ldots, u$, one randomly picks s_i so that the secret key K is equal to the sum of the s_i. Now for each $i = 1, \ldots, u$, a threshold scheme with threshold t_i is used to distribute the shares in s_i to the participants of C_i.

Simmons [45],[47], Brickell [12] and Dawson and Donovan [24] have also listed a number of different methods for constructing compartmented schemes.

7 Prepositioned Schemes

Simmons [46] has also introduced a class of SSSs known as prepositioned schemes. In a *prepositioned* scheme a trusted authority selects a secret key K and an additional piece of information which can be used to indicate the key. As usual he selects n shares in the key K, but this time the shares have the property that when an authorised group of participants pool their shares they require the additional piece of information before they can uniquely determine the key. The shares are distributed when the scheme is set up, however the additional piece of information is withheld until it is necessary to activate the scheme. Using this method one may also deactivate the scheme. This is achieved by changing the secret and determining a new piece of information which indicates the new secret. Once this is done the new secret cannot be recovered until the additional information is once again communicated.

Simmons [46] points out that one relatively easy way of achieving a prepositioned scheme is to select a DES (Data Encryption Standard) key and use it to encode the secret key. The shares are assigned to the DES key as normal and the participants may recover it at any time. When a cipher is received the DES key is used to decrypt it and the plaintext is the secret key which can be used to initiate the appropriate action. However, this scheme is not unconditionally secure. To achieve an unconditionally secure scheme one might select a one–time pad of the same length as the key K and exclusive–or it with K to obtain $K_0 = K \oplus x$. Shares in K_0 may be distributed and K_0 recovered at any time. When K is required x is broadcast and $K_0 \oplus x$ is taken. Alternatively, a scheme may be set up in which the key space is a line L and the share space is a line L' which intersects L at the secret key p, for some point p. In a prepositioned scheme one would withhold the information about the key space. Dawson and Donovan [24] use a similar idea to construct prepositioned schemes based on Shamir's system. Their idea is to choose a polynomial $f(x)$ and the key to be the value $f(x_0)$, for some x_0. The share given to participant P_i is, as usual, $f(i)$. Any t of the participants may use their shares to recover the polynomial. However, the participants cannot recover the secret until the value of x_0 is communicated.

8 Cheaters

McEliece and Sarwate [36] were the first authors to address the problem of a participant cheating. It is conceivable that a participant who enters a false share may prevent the recovery of the secret by the other participants but gain enough information to recover the secret himself. Tompa and Woll [56] point out just how easily this can be achieved. They assume that a SSS based on Shamir's original construction has been implemented. Let K denote the secret key and $f(x)$ denote the polynomial with constant coefficient K. Then each participant P_i, for $i = 1, \ldots, n$, holds the share $f(i)$. If participant P_j wants to cheat, then he can do so by determining a polynomial $g(x)$ of degree at most $t-1$ which satisfies the initial conditions $g(0) = -1$ and $g(i) = 0$, for all $i \neq j$. Such a polynomial can be determined by Lagrange interpolation. When t participants, including participant P_j, concur, participant P_j enters the false share $f(j) + g(j)$ instead of $f(j)$. The system of t linear equations, obtained from these t shares, will have the polynomial $f(x) + g(x)$ as a solution and return the constant coefficient $K - 1$ as the secret key. The remaining $t - 1$ participants may not even know that this is an incorrect value. However, participant P_j does and can in fact recover the secret key for himself. Simmons [44] suggests that this problem may be overcome by determining an additional share to be used to validate the secret key. Other authors have taken a different approach and shown that the mathematical structure of some models can be used to detect cheaters.

McEliece and Sarwate [36] propose a scheme which uses the error correcting capabilities of Reed Solomon codes.

Tompa and Woll [56] suggest an adaptation of Shamir's original scheme. In their proposal the trusted authority selects a number x_i for participant P_i and uses this to calculate the share $f(x_i)$. Now if a group of $t - 1$ participants wants to deceive the

t^{th} participant P_i they must determine a polynomial which has constant coefficient K' distinct from K and which agrees with the value $f(x_i)$ at x_i. The security of their scheme relies on the fact that there is only a very small probability of such a fraud succeeding. This approach will detect that someone has cheated, but will not expose the cheater. For a further discussion of the techniques suggested by Tompa and Woll one may refer to [17].

Karnin, Greene and Hellman [30] suggest that the problem of cheaters can be overcome by the use of a one way function. When the scheme is first set up and the key determined, a one way function may be used to encrypt the key. This encrypted version is placed in a public register. Once the secret is recovered the one way function can be used once again to validate the secret. This method will detect a fraud, but will not detect who is the fraudulent party. To overcome this it has been suggested that the trusted authority also applies the one way function to the shares and places these in the public register. Now if a fraud is detected each share can be verified. However, this scheme is not unconditionally secure as it depends on a one-way function. Simmons [44] discusses a similar approach and suggests that the private pieces of information be partitioned into two parts, the first being the share and the second being a piece of information which can be used to check the consistency with the other inputs. An in depth analysis of these ideas can be found in [44].

In [14] Brickell and Stinson extend these ideas. They suggest that when a participant is given his initial share he is also given a piece of information which he can use to check each of the shares tendered by the other participants. Consider for a moment a simple 2–out–of–n threshold scheme where the key space is a line L in $AG(2, q)$ and the share space a line L' which intersects L at the key p. Let participant P_i hold point p_i. For $j = 1, \ldots, n$ and $j \neq i$, participant P_i is also required to hold a series of $n - 1$ parallel lines $L_{i,j}$, where the line $L_{i,j}$ passes through the share p_j held by participant P_j. At the point of reconstruction of the secret, participant P_i may check that the share tendered by participant P_j is on the line $L_{i,j}$. If participant P_j wants to cheat he must choose a point on each of the lines, $L_{i,j}$ for $1 \leq i \leq n$ where $i \neq j$, held by the other participants. It can be shown that the probability of participant P_j doing this is $1/(q-1)$. Brickell and Stinson extend these ideas to a t–out–of–n threshold scheme, where $t \geq 3$. Here the shares are concealed in hyperplanes and the controller distributes to participant P_i, $n - 1$ parallel hyperplanes together with his share. Brickell and Stinson also discuss how one may deal with a trusted authority who cheats by distributing false shares. Details of this construction are given in [14].

Alternatively, one can use the techniques for verifiable secret sharing schemes to detect cheaters. Chor, Goldwasser, Micali and Awerbuch [20] define a verifiable secret sharing scheme to be a secret sharing scheme in which the participants can verify that they received a valid share in the secret key without having any idea of what the secret is. Verifiable secret sharing schemes are particularly useful in distributed computing where there is a need for protocols for secure multiparty computations, for example procedures such as secret biding, "uninfluenced" voting and distributed coin flipping. The reader is also referred to a paper by Rabin and Ben–Or [39] for more information on verifiable secret sharing schemes.

Other methods for detecting cheaters have been given in [1] and [34].

9 Disenrollment

If one of the participants in a SSS should disclose his share and broadcast it publicly, then obviously the security of the scheme is diminished. Blakley, Blakley, Chan and Massey [9] discuss the possibility of disenrolling that participant and maintaining security at its original level. This is achieved by changing the secret and publicly broadcasting additional information which can be used together with the shares of the remaining participants to determine new shares. The distribution of additional information by a public broadcast overcomes the problems and costs associated with reissuing new shares over a secure channel. Formally, let $K_0, K_1, \ldots, K_L$ denote a set of $L+1$ secrets. Let $s_1, \ldots, s_n$ denote the shares distributed to the participants such that any t of them may use these shares to reconstruct the secret K_0. For $i = 1, \ldots, L$, assume without loss of generality that share s_i is to be neutralised at the i^{th} disenrollment and B_i is the public broadcast at step i. A t–out–of–n threshold scheme is said to have *L–fold disenrollment capability* if given the collection of variables $(K_0, K_1, \ldots, K_L, s_1, \ldots, s_n, B_1, \ldots, B_L)$, then for each $i = 0, \ldots, L$

1. the key K_i can be recovered from any set of t shares selected from the set $\{s_{i+1}, \ldots, s_n\}$ provided that they have the information $B_1, \ldots, B_i$, and

2. the secret cannot be recovered from the information $s_1, \ldots, s_i$, $B_1, \ldots, B_i$ together with any set of $t-1$ or less shares selected from the set $\{s_{i+1}, \ldots, s_n\}$.

Using the *entropy* or "uncertainty" function $H(X)$, (see Shannon [43]), Blakley, Blakley, Chan and Massey give lower bound on the number of bits required to encode a share and show that this grows linearly with the number of possible disenrollments L. If $(K_0, \ldots, K_L, s_1, \ldots, s_n, B_1, \ldots, B_L)$ is a perfect t–out–of–n threshold scheme with L–fold disenrollment capability and $H(K_i) = m$, for $i = 1, \ldots, L$, then

$$H(s_j) \geq (L+1)m \quad \forall j = 1, \ldots, n.$$

Blakley, Blakley, Chan and Massey present two methods for achieving such a scheme. The first of these is given below and is a private communication from Brickell and Stinson. The second scheme is based on geometric configurations.

Let $(K, s_1, \ldots, s_n)$ be a perfect t–out–of–n threshold scheme, where K represents the secret key chosen from $\mathcal{K}$ and s_i represents a share. Then a t–out–of–n threshold scheme with L–fold disenrollment capability $(K_0, \ldots, K_L, \tilde{s_1}, \ldots, \tilde{s_n}, B_1, \ldots, B_L)$ can be constructed from $(K, s_1, \ldots, s_n)$ as follows:

- A set of secret keys $\{K_i \mid i = 0, \ldots, L\}$ is chosen from $\mathcal{K}$.

- For $i = 1, \ldots, n$, $\tilde{s_i}$ is taken to be the share $\tilde{s_i} = (s_i, R_{i,1}, \ldots, R_{i,L})$ where each $R_{i,j}$ is a random binary string of length m.

- When a share $\tilde{s}_i$ is invalidated, a new key K_i is chosen and associated with it are the new shadows $\{s^i_{i+1}, \ldots, s^i_n\}$ that are formed as specified by the original t–out–of–n threshold scheme. The public message B_i which is broadcast through a public channel consists of the union of the $R_{j,i}$ with the s^i_j. So B_i is

$$\{R_{i+1,i} + s^i_{i+1}, \ldots, R_{n,i} + s^i_n\}.$$

Participant P_j has been given $R_{i,i}$ originally and therefore can recover s^i_j.

They also show that the t–out–of–n perfect threshold scheme with L–fold disenrollment capability constructed above achieves the lower bound $H(s_j) = (L+1)m$, for $j = 1, \ldots, n$.

Dawson and Donovan [24] use these techniques to construct a scheme with disenrollment capability based on Shamir's system. This construction will be described below. Assume that it is necessary to set up a t–out–of–n threshold scheme with L–fold disenrollment capabilities. Initially, a trusted authority selects $L+1$ secrets $K_0, K_1, \ldots, K_L$ from the set Z_q as well as selecting $L+1$ polynomials $f_i(x)$ of degree $t-1$, for $i = 0, \ldots, L$, where K_i is the constant coefficient of $f_i(x)$. The trusted authority generates n shares for each of the $L+1$ secrets. Participant P_j's share of secret K_i is s_{ji}, where $f_i(j) = s_{ji}$. Numbers r_{ji}, for $j = 1, \ldots, n$ and $i = 1, \ldots, L$, are selected at random from Z_q. The number r_{ji} is combined with the share s_{ji} modulo q to form s'_{ji}; that is, $s'_{ji} = s_{ji} + r_{ji} \pmod{q}$. In this manner, the number r_{ji} is used to mask the share s_{ji}. Initially, the trusted authority sends, over a secure channel, the $L+1$ shares s_{j0} and s'_{ji}, for $i = 1, \ldots, L$, to participant P_j. This process is repeated for each participant. In the first instance any t participants can use their shares, of the form s_{j0}, and derive the secret K_0. However, if one of the participants reveals his shares (assume for simplicity of notation that it is the first participant) the trusted authority can disenroll this person. This is achieved by the following procedure. The trusted authority changes the key to K_1 and broadcasts, on an open channel, the numbers r_{j1}, for $j = 2, \ldots, n$. Participant P_j, can use the number r_{j1} to unmask s'_{j1} and recover the share s_{j1} to secret K_1. Hence any t of the remaining $n-1$ participants can combine their shares and derive K_1. However, without knowledge of r_{11}, the disenrolled participant is not able to derive share s_{11}. Hence, this person can no longer participate in the scheme. This procedure can be repeated and L participants can be disenrolled, assuming that $n - L \geq t$.

It should be noted that as well as disenrollment, the above scheme provides a method whereby a trusted authority can establish a new secret at any time. The key can be changed and the information, required to change the shares, broadcast on an insecure channel. Schemes with this regeneration property have been termed *l–span* general SSSs, and an alternative method for their construction is given by Harn and Lin in [26]. Chaum devotes the paper [18] to a similar process. It should also be noted that Simmons' prepositioned schemes also have this capability.

10 Conclusion

Shamir's and Blakley's original papers have generated much interest, from both a theoretic and applied point of view. Since 1979 many papers have appeared on the topic. These papers come under the broad headings of: 1) mathematical structures used to model SSSs; 2) adaptations which can be used to meet many of the needs of the real world community; 3) maintaining the flexibility and security of a SSS; 4) the study of the information rate of a SSS. An overview of these topics has been presented in this paper.

Acknowledgement

This research was supported by the ARC, the QUT Meritorious Grants Projects Scheme, ATERB and carried out while the author was a Postdoctoral Fellow at the Queensland University of Technology. I wish to thank sincerely Sheila Oates-Williams, Ed Dawson and the referee for their comments in relation to the manuscript and Bill Caelli for his support.

References

[1] Charles Asmuth and John Bloom, *A modular approach to key safeguarding*, IEEE Trans. on Inform. Theory, **29**, (1983), 208–210.

[2] Amos Beimel and Benny Chor, *Universally Ideal Secret Sharing Schemes*, in Lecture Notes in Computer Science 740; Advances in Cryptology: Proc. Crypto '92, Santa Barbara, CA, Aug. 1992, Berlin: Springer–Verlag, (1992), 185–197.

[3] Josh Benaloh and Jerry Leichter, *Generalized secret sharing and monotone functions*, in Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88, S. Goldwasser Ed., Santa Barbara, CA, Aug. 1988, Berlin: Springer–Verlag, (1990), 27–35.

[4] Michael Bertilsson and Ingemar Ingemarsson, *A construction of practical secret sharing schemes using linear block codes*, Abstracts Auscrypt '92, Gold Coast, Aust., Dec. 1992, 2-21–2-26.

[5] Albrecht Beutelspacher, *Enciphered geometry: some application of geometry to cryptography*, Proc. Combinatorics '86, in Annals of Discrete Mathematics, **37**, A. Barlotti, M. Marchi and G. Tallini Eds., Amsterdam: North Holland, (1988), 59–68.

[6] A. Beutelspacher and K. Vedder, *Geometric structures as threshold schemes*, 1986 IMA Conference on Cryptography and Coding, Cirencester, England, in Cryptography and Coding, H.J. Beker and F.C. Piper Eds., Oxford: Clarendon Press, (1989), 255–268.

[7] A. Beutelspacher, *How to say "no"*, in Lecture Notes in Computer Science 434; Advances in Crytpology; Proc. Eurocrypt '89, J.-J Quisquater and J. Vandewalle Eds., Houthalen, Belgium, 1989, Springer–Verlag, (1989), 491–496.

[8] G.R. Blakley, *Safeguarding cryptographic keys*, Proc. AFIPS 1979 Natl. Computer Conf., New York, **48**, (1979), 313–317.

[9] Bob Blakley, G.R. Blakley, Agnes Hui Chan and James L. Massey, *Threshold schemes with disenrollment*, in Lecture Notes in Computer Science 740; Advances in Cryptology: Proc. Crypto '92, Santa Barbara, CA, Aug. 1992, Berlin: Springer–Verlag, (1992), 546–554.

[10] C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, *Graph decompositions and secret sharing schemes*, in Lecture Notes in Computer Science 658; Advances in Cryptology: Proc. of Eurocrypt '93, Hungary, May 1992, Berlin: Springer–Verlag, (1993), 1–24.

[11] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, *On the information rate of secret sharing schemes*, in Lecture Notes in Computer Science 740; Advances in Cryptology: Proc. Crypto '92, Santa Barbara, CA, Aug. 1992, Berlin: Springer–Verlag, (1992), 149–169.

[12] E.F. Brickell, *Some ideal secret sharing schemes*, J. Combinatorial Math. and Combinatorial Computing, **6**, (1989), 105–113.

[13] E.F. Brickell and D.M. Davenport, *On the classification of ideal secret sharing schemes*, J. Cryptology, **4**, (1991), 123–134.

[14] E.F. Brickell and D.R. Stinson, *The detection of cheaters in threshold schemes*, Siam J. on Discrete Math., **4**, (1991), 502–510.

[15] E.F. Brickell and D.R. Stinson, *Some improved bounds on the information rate of perfect secret sharing schemes*, J. Cryptology, **5**, (1992), 153–166.

[16] R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, *On the size of shares for secret sharing schemes*, in Lecture Notes in Computer Science 576; Advances in Cryptology: Proc. of Crypto '91, J. Feigenbaum Ed., Santa Barbara, CA, Aug. 1991, Berlin: Springer–Verlag, (1992), 101–113.

[17] Marco Carpentieri, Alfredo De Santis and Ugo Vaccarp, *Size of shares and probability of cheating in threshold schemes*, Proc. Eurocrypt '93, Lofthus, May 1993, M97–M102.

[18] David Chaum, *How to keep a secret alive: extensible partial key, key safeguarding and threshold systems*, in Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84, G.R. Blakley and D. Chaum Eds., Santa Barbara, CA, Aug. '84, Berlin: Springer–Verlag, (1985), 481–485.

[19] D. Chen and D.R. Stinson, *Recent results on combinatorial constructions for threshold schemes*, Australas. J. Combin., **1**, (1990), 29–48.

[20] Benny Chor, Shafi Goldwasser, Silvio Micali and Baruch Awerbuch, *Verifiable secret sharing and achieving simultaneity in the presence of faults*, Proc. 26th IEEE Symp. Found. Comp. Sci., Portland OR, (1985), 383–395.

[21] Benny Chor and Eyal Kushilevitz, *Secret sharing over infinite domains*, in Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto '89, G. Brassard Ed., Santa Barbara, CA, Aug. 1989, Berlin: Springer–Verlag, (1990), 299–306.

[22] Joan Cooper, Diane Donovan and Jennifer Seberry, *Secret sharing schemes arising from latin squares*, (submitted).

[23] E. Dawson, E.S. Mahmoodian and Alan Rahilly, *Orthogonal arrays and ordered threshold schemes*, Australasian Journal of Combinatorics, **8**, (1993), 27–44.

[24] Ed Dawson and Diane Donovan, *Shamir's scheme says it all*, Proc. of IFIP/Sec '93, Toronto, Canada, May 1993, 69–80.

[25] D.E. Denning, Cryptography and Data Security, Addison–Wesley, (1982).

[26] Lein Harn and Hung–Yu Lin, *An l–span generalized secret sharing scheme*, in Lecture Notes in Computer Science 740; Advances in Cryptology: Proc. Crypto '92, Santa Barbara, CA, Aug. 1992, Berlin: Springer–Verlag, (1992), 604–606.

[27] I. Ingemarsson and G.J. Simmons, *A Protocol to set up shared secret schemes without the assistance of a mutually trusted party*, in Lecture Notes in Computer Science 473; Advances in Cryptology, Proc. Eurocrypt '90, I. Damgård Ed., Aarhus, Denmark, May 1990, Berlin: Springer–Verlag, (1991), 266–282.

[28] M. Ito, A. Saito and T. Nishizeki, *Secret sharing scheme realising general access structure*, Proc. IEEE Global Telecommun. Conf., Globecom '87, Tokyo, (1987), 99–102. Also appeared in Trans. IECE Japan, **J71-A** 1988.

[29] Wen–Ai Jackson and Keith M. Martin, *On ideal secret sharing schemes*, (submitted).

[30] Ehud D. Karnin, Jonathan W. Greene and Martin E. Hellman, *On secret sharing systems*, IEEE Intl. Symp. Inform. Theory, Santa Monica, CA, February 1981, IEEE Trans. Inform. Theory, **IT–29**, No 1, (1983), 35–41.

[31] S.C. Kothari, *Generalized linear threshold scheme*, in Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84, G.R. Blakley and D. Chaum Eds., Santa Barbara, CA, Aug. 1984, Berlin: Springer–Verlag, (1985), 231–241.

[32] Kaoru Kurosawa, Koji Okada and Keiichi Sakano, *Nonperfect secret sharing schemes and matroids*, Proc. Eurocrypt '93, Lofthus, May 1993, M104–M120.

[33] Chi Sung Laih, Jau Yien Lee and Lein Harn, *A new threshold scheme and its application in designing the conference key distribution cryptosystem*, Infor. Processing Lett., **32**, (1989), 95–99.

[34] Hung–Yu Lin and Lein Harn, *A generalized secret sharing scheme with cheater detection*, Proc. Asiacrypt '91, Nov. 1991, Japan, 83–87.

[35] Keith M. Martin, *New secret sharing schemes from old*, (submitted).

[36] R.J. McEliece and D.V. Sarwate, *On sharing secrets and Reed–Solomon codes*, Commun. ACM, **24**, No 9, (1981), 583–584.

[37] Maurice Mignotte, *How to share a secret*, Workshop on Cryptography, Burg Feuerstein, Germany, March 1982, in Cryptography, **149**, T. Beth Ed., Berlin: Springer–Verlag, (1983), 371-375.

[38] Christine M. O'Keefe, *Applications of finite geometries to information security*, Australasian Journal of Combinatorics, **7**, (1993), 195–212.

[39] Tal Rabin and Michael Ben–Or, *Verifiable secret sharing and multiparty protocols with honest majority*, Proc. 21st. ACM Symposium on the Theory of Computing, (1990), 73–85.

[40] P.J. Schellenberg and D.R. Stinson, *Threshold schemes from combinatorial designs*, J. Combin. Math. and Comb. Comp., **5**, (1989), 143–160.

[41] P. D. Seymour, *On secret sharing matroids*, Journal of Combin. Theory B, **56**, (1992), 69–73.

[42] A. Shamir, *How to share a secret*, Commun. A.C.M., **22**, No 11, (1979), 612–613.

[43] C.E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, (1948), 656–715.

[44] G.J. Simmons, *Robust shared secret schemes or 'how to be sure you have the right answer even though you don't know the question'*, Congressus Numerantium, **68**, (1989), 215–248.

[45] G.J. Simmons, *How to (really) share a secret*, in Lecture Notes on Computer Science 403; Advances in Cryptology: Proc. Crypto '87, S. Goldwasser Ed., Santa Barbara, CA, 1987, Berlin: Springer–Verlag, (1990), 390–448.

[46] G.J. Simmons, *Prepositioned shared secret and/or shared control schemes*, in Lecture Notes on Computer Science 434; Advances in Cryptology: Proc. Eurocrypt '89, J.J. Quisquater and J.Vanderwalle Eds., Houthalen, Belgium, April 1989, Berlin: Springer–Verlag, (1990), 436–467.

[47] G.J. Simmons, *An Introduction to shared secret and/or shared control schemes and their applications*, in Contemporary Cryptology, The Science of Information Integrity, IEEE Press, Piscataway, (1991), 441–497.

[48] G.J. Simmons, Wen–Ai Jackson and Keith Martin, *The geometry of shared secret schemes*, Bull. of the ICA, **1**, (1991), 71–88.

[49] G.J. Simmons, *Geometric shared secret and/or shared control schemes*, in Lecture Notes on Computer Science 537; Advances in Cryptology: Proc. Crypto '90, A.J. Menezes and S.A. Vanstone Eds., Santa Barbara, CA, 1990, Berlin: Springer–Verlag, (1991), 216–241.

[50] D.R. Stinson and S.A. Vanstone, *A combinatorial approach to threshold schemes*, SIAM J. on Discrete Math., **1**, (1988), 230–236.

[51] D.R. Stinson, *An explication of secret sharing schemes*, Designs, Codes and Cryptography, **2**, (1992), 357–390.

[52] D.R. Stinson, *New general bounds on the information rate of secret sharing schemes*, in Lecture Notes in Computer Science 740; Advances in Cryptology: Proc. Crypto '92, Santa Barbara, CA, Aug. 1992, Berlin: Springer–Verlag, (1992), 170–184.

[53] D.R. Stinson, *Combinatorial designs and cryptography*, L.M.S. Lecture Notes Series 187, Surveys in Combinatorics, Ed. K. Walker, (1993), 257–287.

[54] D.R. Stinson, *Decomposition constructions for secret sharing schemes*, IEEE Trans. Inform. Th., (to appear).

[55] Anne Penfold Street and Deborah J. Street, Combinatorics Of Experimental Design, Clarendon Press, Oxford, (1987).

[56] Martin Tompa and Heather Woll, *How to share a secret with cheaters*, J. of Cryptology, **1**, (1988), 133–138.

[57] D.J.A. Welsh, Matroid Theory, Academic Press, London, (1976).

[58] W.D. Wallis, *Not all perfect extrinsic secret sharing schemes are ideal*, Australasian Journal of Combinatorics, **2**, (1990), 237–238.

(Received 22/12/92; revised 13/8/93)